ABSTRACT OF THE DISCLOSURE

[00125] A computing platform (10) protects system firmware (30) using a manufacturer certificate (36). The manufacturer certificate binds the system firmware (30) to the particular computing platform (10). A secure run-time platform data checker (200) and a secure run-time checker (202) check the system firmware during operation of the computing platform (10) to ensure that the system firmware (30) or information in the manufacturer certificate (36) has not been altered. Application software files (32) and data files (34) are bound to the particular computing device (10) by a platform certificate (38). Access to certain configurations of the device, such as access to a test configuration is initiated by entering a password. The password is encrypted through a hashing process to reduce its size and compared to an access code that has been hashed and stored on the computing platform.